f 4,-

HACK-TIC

#2

TIJDSCHRIFT VOOR TECHNO-ANARCHISTEN

Met in dit nummer:

- **Autotelefoonnet 1 gehackt**
- **Gratis bellen in cellen**
- **AKZO gehackt**
- **Telefoonfraude te makkelijk**
- **Cursus UNIX hacking**
- **Lijst snelheidscontrolepunten**



Nederlands Grootste, Dikste, Voordeligste en Kleurrijkste Hacker-blad

COLOFON

HACK-TIC: is Nederlands eerste hacker-blad. Naar we hopen verschijnt het ongeveer 10 x per jaar.

UITGAVE: met moeite (door een volkomen ongebonden en ongeorganiseerd gezelschap van vreemde types).

REDAKTIE: The Key, John D., Tx, Herman Acker, Peter Poelman en Rop.

ILLUSTRATIES: Koen Hottentot.

KONTAKT: De redaktie is te bereiken via **p.b. 22953, 1100 DL Amsterdam.** UUCP: **...!mcvax!neabbs!rop.** Op het FIDO net **2:280/1 Hack Tic.** Telex (modem 50 baud telecommunicatiecomfort van de PTT) **12969 neabs nl**, telefax **020-763706.** Zowel bij telex als bij fax even vermelden dat het voor Hack-Tic is. Abonnees die er in slagen de redaktie telefonisch (voice) te bereiken moeten met sancties rekening houden.

PRIJS: Losse nummers kosten 4 gulden, een abonnement voor 10 nummers (moet ongeveer een jaar meegaan) kost *f* 37,50. Abonnementsgelden overmaken op bankrekeningnummer **98.72.84.541** t.n.v. Rop Gonggrijp. Rekening loopt bij de verenigde spaarbank, postrek. no. **15368.** Abonnementen beginnen met het laatst uitgegeven nummer tenzij je bij de betaling een ander beginnummer aangeeft. Oude nummers die niet meer voorradig zijn worden ook niet in rekening gebracht.

PRIVACY: Het is waar: als 'ze' willen, hoeven ze alleen maar naar onze bankafschriften te kijken om te zien wie er abonnee zijn. Wij vinden Hack-Tic een uiterst onschuldig blaadje, maar de kans bestaat dat lokale, regionale, nationale en in de toekomst wellicht zelfs Europese overheden het daar niet mee eens zijn. Heb je een maatschappelijke positie die je niet wilt verliezen dan kun je ook geld en adres bijsluiten in een envelop en die aan onze postbus sturen, wij weten dan genoeg (jaja, als ze de post open maken ben je nog steeds de pisang). De Hack-Tic wordt altijd verstuurd in een neutrale envelop. (Straks denkt je hospita nog dat je porno koopt per postorder). Hack-Tic is ook verkrijgbaar bij de goede boekhandel (wellicht herkenbaar aan het observatieteam voor de deur).

DISCLAIMER: Informatie in Hack-Tic dient slechts een educatief doel. Gebruik van deze informatie zou strafbaar/staatsgevaarlijk/stout kunnen zijn. De redaktie wijst iedere verantwoordelijkheid voor gebruik door lezers van de in Hack-Tic opgenomen informatie af.

NADRUK: toegestaan! Kranten, tijdschriften, omroepstichtingen, politieke partijen, wasmachinereparateurs etc. etc. mogen zonder voorafgaande toestemming van de redaktie (maar natuurlijk met bronvermelding) stukken overnemen uit de Hack-Tic. De bovenstaande disclaimer blijft echter van kracht. Nadruk van de gehele Hack-Tic is natuurlijk verboden. (Neem toch maar een abonnement, want wij hebben hier een kooi vol goeie advokaten die al weken niets meer gegeten hebben.)

NABESTELLEN: Oude nummers kosten ook fl. 4,- en kunnen via de redaktie-postbus besteld worden.

HOE: Hack-Tic werd met het WYSMRWYG (What You See Might Resemble What You Get) DTP pakket Ventura 1.1 gemaakt op een gammele AT. Print-outs van elke pagina werden gemaakt met een EPSON RX-80 en daarna verkleind en gefotokopieerd. Dan nog een nietje d'r in en klaar was Kees (hopen we terwijl we dit tikken).

VERKRIJGBAAR: o.a. bij Het Computercollectief, Fort van Sjakoo en Athenaeum Boekhandel, allen in Amsterdam en verder bij elke goede boek- of tijdschriftenhandel.

VRAAG naar Hack-Tic!

Techno-Anarchisten

De redaktie van Hack-Tic verwerpt geweld, in welke vorm dan ook en wijst terreurdaden af. Wij zijn tegen bewapening en hopen op meer begrip tussen de volken op deze planeet voor het te laat is.

Waarom gaan we ons te buiten aan dit soort pathetische statements? Omdat je met terroristen wordt vergeleken zodra je zegt dat je anarchist bent. En daar we Hack-Tic een tijdschrift voor techno-anarchisten hebben genoemd zouden we dus zelf wel een groepje door Moskou betaalde oproerkraaiers zijn.....

Dit was in ieder geval de mening van een (gelukkig erg klein) gedeelte van de bezoekers van een beurs waarop we probeerden om de Hack-Tic aan de man/vrouw te brengen.

Voor ons is een anarchist heel simpel een persoon die iedere vorm van gezag afwijst. Een techno-anarchist is dus een technicus die geen gezag erkent. Hij/zij weigert slaafs te doen wat de computerwereld zegt. Hij/zij weigert mee te werken aan het opbouwen van informatiemonopolies.

Maar hij/zij weigert niet alleen maar, maar werkt ook actief aan een alternatief gebruik van de techniek. De techno-anarchist ondersteunt het opbouwen van eigen, goedkope netwerken om te dienen als alternatief voor veel te dure, door de overheid opgezette (computer)netwerken. De techno-anarchist wil inzicht hebben in alle informatie die burgers aangaat en als hij/zij die niet krijgt dan zijn een modem en een computer genoeg om die informatie zelf te gaan halen.

Het techno-anarchisme is er voor iedereen die vrij met techniek wil omgaan. Wie de Hack-Tic ziet als een blad voor 'Hi-Tech Hells Angels' heeft het niet begrepen!

Hoewel het gebruik van veel van de in Hack-Tic beschreven technieken strafbaar is (of zal worden), is het nooit echt gevaarlijk. In Hack-Tic zul je geen handleidingen voor het maken van bommen of wapens aantreffen. Want hoewel de redaktie over veel dingen van mening verschilt zijn we het er over eens dat geweld een tamelijk primitieve manier is om conflicten op te lossen en dat er zelfs voor hooglopende meningsverschillen creatievere manieren zijn om de zaak op te lossen.

Nog iets: Als je bijvoorbeeld de autotelefooninformatie in dit nummer gebruikt om rijk aan te worden (wij zullen niet ontkennen dat er geld mee te verdienen is), dan moet je dat zelf weten. Als je gepakt wordt moet je het dan echter ook zelf weten. Als je de techniek alleen zelf gebruikt en niet commercieel benut en je wordt opgepakt, dan staat de redaktie achter je. Jammer dat de redaktie niet beschikt over de (financieële) middelen om dan ook werkelijk iets voor je te betekenen, dus wees toch maar voorzichtig.

We doen meer telecommunicatie dan de telefoon bij u thuis

OPLEIDING TOT TELECOMMUNIST

deel 2

Door Peter Poelman en The Key

Bellen in de auto; voor velen een noodzaak, voor nog veel meer een statussymbool. Voor slechts enkelen een schitterende manier om geld te kloppen uit de zakken van graag betalende yups, en voor een wel zeer selecte groep de perfecte hack.

Autotelefoonnet 1



Momenteel zijn er in Nederland maar liefst 3 systemen in gebruik, bij gebrek aan fantasie genaamd autotelefoon 1, 2 en 3. Net 1 benut frequenties in de normale mobilofoonband, die zijn dus met een scanner te ontvangen. Net 2 werkt voor het overbrengen van de gegevens met een 1200 baud full-duplex verbinding (niet exact hetzelfde als in een V22 modem), ergens op de 400 MHz. Net 3 draait nog maar pas (rond de 900 MHz). We gaan het in dit artikel alleen hebben over het eerste autotelefoonnet, kortweg ATF1.

De makers van dit eerste autotelefoonnet namen het met de veiligheid nog niet zo nauw: er is geen enkele code of wat dan ook in het prototcol ingebouwd, het hele zaakje is zo lek als een mandje!

ATF is een full-duplex systeem: dat wil zeggen dat er tegelijkertijd gesproken en geluisterd kan worden. Dit wil weer zeggen dat er voor een gesprekskanaal twee frequenties zijn gereserveerd.

De ene frequentie noemen we het basiskanaal: hierop zendt de steunzender van het autotelefoonnet. Deze steunzenders staan door het hele land opgesteld en zijn via een directe lijn verbonden met de BTD (Bijzonder Tellende Diensten) ofwel 06-centrale in Rotterdam. De andere frequentie noemen we het mobiele kanaal; hierop zendt het voertuig (niet altijd een auto; ook binnenschippers maken veel gebruik van ATF1).

Tabel 1 bevat een lijstje met gebruikte frequenties

Zoals je ziet liggen de frequenties steeds 0.03 MHz verder. Ook ligt het mobiele kanaal steeds 4.6 MHz lager dan het bijbehorende basiskanaal.

Als je met de scanner luistert naar de basiskanalen vallen een aantal dingen op:

Er zit op de basiskanalen (als er geen gesprek is) constant een datariedel in de lucht. Deze riedel geeft het nummer van de regio aan en is verder niet interessant.

Hinderlijk is hij echter wel, want hij maakt het onmogelijk om gesprekken te scannen, daar er constant een signaal is.

Door "overspraak" komt er altijd wel wat van wat de automobilist zegt op het basiskanaal terecht, je hoeft dus geen twee scanners te hebben om toch het hele gesprek te kunnen volgen.

Op de mobiele kanalen hoor je zo nu en dan (voor een gesprek tot stand komt) een flinke datariedel.

De elementen voor deze datariedel staan in Tabel 2

Zoals je ziet zijn de eerste 5 bits steeds gelijk. Verder is bij de cijfers een spiegelbeeld te zien: Het tweede blok is het spiegelbeeld van het vierde stuk. Het is echter mogelijk om de "kop" van het ene getal en de "staart" van het andere uit te zenden: je kunt dan in een telegram twee getallen kwijt; de spiegelwerking is dan weg.

Dit wordt gedaan om (in de oproep) het kanaalnummer mee te geven, en om de "kanaal-beschikbaar"-riedel samen te stellen. De riedels ontstaan door de benodigde telegrammen botweg aan elkaar vast te knopen tot een lange reep piepjes, dus ZONDER tussenpozen.

Snap je er al lang niets meer van? Een paar voorbeelden:

Gesprek telefoonnet - autotelefoon:

Op kanaal 19 komt de basis in de lucht, en begint gelijk te riedelen:

0111010100000101	1
0111010010001001	2
0111010001010001	3
0111001100000110	4
0111001010001010	5
0111010100000110	14

dan verdwijnt de basis weer.

Deze riedel wil zeggen: Autotelefoon 12345, er is een gesprek voor U op kanaal 14. (Let op: die 14 is dus een dubbel cijfer, de spiegelwerking in het telegram is verstoord).

De betreffende autotelefoon moet nu als de sodemieter naar kanaal 14, om daar in de lucht te komen met een aanhoudende toon van 1950 Hz (de 1 dus). De centrale bevestigt dit op haar kanaal door ook een 1950 Hz piep uit te zenden. Ondertussen gaat de bel van de autotelefoon en hoort de abonnee aan het telefoonnet de rinkeltoon. Als de autotelefoon niet binnen enkele seconden op het kanaal is krijgt de abonnee een bandje met "Met de door U gekozen autotelefoon kan op dit moment geen verbinding worden gemaakt".

Maar goed: de bel gaat over. Binnen 1 minuut wordt er opgepakt (zo niet, dan geeft de centrale het op). Dit geeft de autotelefoon aan door het hoge piepje (2070 Hz) kort uit te zenden. vanaf dit moment kan het gesprek beginnen.

Geeft dan wel de autotelefoon, dan wel de centrale het canceltelegram, dan is de verbinding weg. (Let wel: de centrale blijft net zo lang afsluiten tot je ook daadwerkelijk uit de lucht bent).

Gespek autotelefoon - telefoonnet:

De autotelefoon zoekt een vrij kanaal. Op dit kanaal wordt door de centrale constant het zelfde telegram uitgezonden. Het bestaat uit een dubbel cijfer, het eerste stuk is altijd een 9, het tweede geeft het nummer van de regio (dus niet van het kanaal). Amsterdam is bijvoorbeeld regio 5. In Amsterdam staat er dus op een vrij kanaal:

0111000011001010 0111000011001010 etc. etc.

De autotelefoon onderbreekt dit signaal door in de lucht te komen en eerst een 600 msec piep van 2070 Hz te geven. Daarna komt de riedel, b.v.:

M Start-1-2-3-4-5-2-0-7-1-7-6-6-6-Stop-
B 1-2-3-4-5

M Start-1-2-3-4-5-2-0-7-1-7-6-6-6-Stop
B 1-2-3-4-5

M=Mobiel kanaal B=Basiskanaal

Dit voorbeeld wil zo veel zeggen als: Autotelefoon 12345 hier, ik wil bellen met 020-717666. Let er op dat de eerste nul van het telefoonnumer niet wordt uitgezonden. Het twee keer (zonder tussenpauze) uitzenden van de hele riedel is niet nodig, maar de echte autotelefoons doen het wel. Na de laatste stop komt de vebinding tot stand.

Op de onderste regel zie je dat de centrale, zodra je je eigen nummer hebt uitgezonden, dit herhaalt om vergissingen uit te sluiten (maar niemand zegt dat je daar naar moet luisteren)...

Gaat de centrale na het herhalen van het nummer cancelen (achter elkaar het cancel telegram uitzenden tot je uit de lucht bent), dan is het autotelefoonnummer wat je gebruikt afgesloten.

Gebruik

Internationaal bellen via ATF1 is vanuit Nederland niet meer mogelijk. Dit hangt samen met het feit dat een complete bende slimme jongens gestolen en grijs geimporteerde autotelefoons verkocht waarvan je het nummer zelf kon instellen (zat in eprommetjes of zelfs op draadbruggetjes in het toestel). Als je dicht genoeg bij de Duitse grens woont kun je echter via de Duitse steunzenders gratis met de hele wereld bellen.

Het gesprek hoeft niet noodzakelijk full-duplex te zijn, je mag 10 sec. uit de lucht voor de centrale het gesprek beeindigt, die 10 sec. kun je dus gebruiken om te luisteren, zodat je in principe aan een zend-ontvanger genoeg hebt. De klus is dus om een computerprogramma te maken dat de riedels samenstelt.

Tabel 1: Rieideltjes ATF 1

Deze datariedels zijn opgebouwd uit datatelegrammen van 16 bits. Elke bit duurt 10 milliseconden. Een 1 staat voor een pieptoon van 1950 Hz, een 0 voor een pieptoon van 2070 Hz.

Starttelegram	01110 01000100010
Stoptelegram	01110 10000100001
Canceltelegram	01110 10101010101
Cijfer 0	01110 11000 0 00011
Cijfer 1	01110 10100 0 00101
Cijfer 2	01110 10010 0 01001
Cijfer 3	01110 10001 0 10001
Cijfer 4	01110 01100 0 00110
Cijfer 5	01110 01010 0 01010
Cijfer 6	01110 01001 0 10010
Cijfer 7	01110 00110 0 01100
Cijfer 8	01110 00101 0 10100
Cijfer 9	01110 00011 0 11000

Tussen de verschillende bits zitten geen pauzes. De spaties hebben we er alleen maar tussen gezet om de structuur van het geheel duidelijk te maken.

Het lijkt me nodeloos te zeggen dat het uiterst illegaal is om met een niet goedgekeurde zender uit te zenden (soms echter best leuk). Verder is het niet toegestaan (en moreel niet helemaal netjes) om op andermans autotelefoonnummer te bellen.

De PTT heeft echter een mobiele telefoonwinkel en die heeft ook telefoon.......

Tabel 2: kanalen ATF 1

Kanaal	Basis	Mobiel	Locatie
1	153.0100	148.4100	Goes, Utrecht, Smilde
2	153.0300	148.4300	Maastricht, Rotterdam, Ugchelen
3	153.0500	148.4500	Rotterdam, Ugchelen
4	153.0700	148.4700	Venlo, Utrecht
5	153.0900	148.4900	Test- en demonstratiekanaal
6	153.1100	148.5100	Den Haag, Ugchelen
7	153.1300	148.5300	Den Haag, Maastricht, Megen, Tjerkgaast
8	153.1500	148.5500	Rotterdam, Zwollerkerspel
9	153.1700	148.5700	Leeuwarden, Mierlo, Utrecht
10	153.1900	148.5900	Rotterdam, Zwollerkerspel
11	153.2100	148.6100	Amsterdam, Mierlo, Smilde
12	153.2300	148.6300	Rotterdam, Megen, Alkmaar
13	153.2500	148.6500	Amsterdam, Mierlo, Goes
14	153.2700	148.6700	Maastricht, Megen, Rotterdam, Tjerkgaast
15	153.2900	148.6900	Den Haag, Zwollerkerspel
16	153.3100	148.7100	Amsterdam, Roosendaal, Smilde
17	153.3300	148.7300	Alkmaar, Rotterdam, Ugchelen, Venlo
18	153.3500	148.7500	Wieringerwerf, Rotterdam, Markelo
19	153.3700		OPROEPKANAAL
20	153.3900	148.7900	Markelo, Mierlo, Rotterdam, Wieringerwerf
21	153.4100	148.8100	Den Haag, Leeuwarden
22	153.4300	148.8300	Lelystad, Loon op Zand
23	153.4500	148.8500	Rotterdam, Winschoten, Alkmaar
24	153.4700	148.8700	Lelystad, Loon op Zand, Winschoten
25	153.4900	148.8900	Leeuwarden, Utrecht, Venlo
26	153.5100	148.9100	Groningen, Den Haag, Ugchelen
27	153.5300	148.9300	Groningen, Amsterdam
28	153.5500	148.9500	Lelystad, Rotterdam, Venlo
29	153.5700	148.9700	Megen, Coevorden, Wieringerwerf, Rotterdam
30	153.5900	148.9900	Maastricht, Roosendaal, Megen, Tjerkgaast
31	153.6100	149.0100	Amsterdam, Roosendaal, Coevorden, Venlo
32	153.6300	149.0300	Groningen, Megen, Tjerkgaast
33	153.6500	149.0500	Alkmaar, Loon op Zand, Winschoten
34	153.6700	149.0700	Amsterdam, Roosendaal, Coevorden
35	153.6900	149.0900	Rotterdam, Zwollerkerspel
36	153.7100	149.1100	Goes, Markelo, Mierlo, Utrecht, Amsterdam
37	153.7300	149.1300	Alkmaar, Loon op Zand, Maastricht

De aangegeven frequenties zijn in MHz.

UNIX, the hack way (part 1)

Het UNIX operating system

UNIX is een multi-user operating systeem dat bijna op alle grote computers te draaien is. Het is een mooi, gebruikersvriendelijk (en dus hackersvriendelijk) systeem, erg leuk speelgoed. Je kunt UNIX ook op je PC draaien (dan heet het XENIX).

UNIX is oorspronkelijk ontwikkeld door Bell labs, het laboratorium van AT&T. De UNIX Research Group onder leiding van Ken Thompson bracht de UNIX Versions 1 t/m 7, allemaal redelijk primitieve UNIXen en het begon pas echt toen in 1980 UNIX System III op de markt kwam, een uitgave ondersteund door de User Support Group binnen AT&T, die veel commercieler en gebruikersgerichter tegen de zaken aankeek.

Dit System III is eigenlijk een aangepaste Version 7. Inmiddels (sinds 1983) wordt er meestal gewerkt met UNIX System V. De UNIX System I, II en IV zijn alleen intern in gebruik geweest en die zul je dus "op straat" niet tegenkomen. Van de Research Group is inmiddels een UNIX Version 8, maar om wille van de standaard wordt deze slechts spaarzaam aan onderwijsinstellingen ter beschikking gesteld.

Terwijl dit alles bij AT&T plaatsvond was de rest van de wereld ook in beweging, want door de lage licentieprijzen die AT&T aan onderwijsinstellingen rekende, kwamen er ook andere "UNIXen" op de markt, allemaal toegespitst op een bepaald gebied. In al deze ontwikkelingen speelde de Berkeley universiteit in Californie een grote rol. Zo ontwikkelde BSD (Berkeley Software Distributies) een UNIX met veel extra's. Het systeem wordt (vaak) gebruikt op de hardware van DEC (Digital Equipment Corporation), zo is er de BSD 2.x voor de PDP-11 en de BSD 4.x voor de Vax.

Het bedrijfsleven kreeg ook interesse en veel software-huizen kochten een licentie op UNIX om er lekker aan te kunnen sleutelen, en als er iets commercieel bruikbaars uitkwam werd het op de markt gegooid. Omdat UNIX door AT&T was vastgelegd kregen we Ultrix, Munix, Sinix, UX, Onyx en Xenix. Het laatste systeem is van Microsoft, een iets verkleinde versie van UNIX dat ook op IBM PC's draait. De nieuwste ontwikkeling is dat AT&T en SUN (waar veel ex-BSD'ers van Berkeley werken) samen een versie op de markt gaan brengen die de absolute standaard moet worden. Als gebruiker (kraker) merk je echter weinig van deze puinhoop, en het enige belang van het Versie-, System- of ander nummer ligt in de fouten die er in de beveiliging van oudere systemen zitten.

Genoeg geluld, aan de slag.

Als je het systeem aan de lijn krijgt meldt het zich in een paar regels, en vervolgens vraagt het "login: ", en als hierop iets wordt geantwoord, vervolgt het met "Password: ". Wat je hierop intikt echo't hij niet. Als een van de twee fout is volgt de mededeling "Login incorrect". Meestal mag je het zo vaak proberen als je wilt, maar je hebt ze ook die na drie keer neerleggen. Er zijn in Nederland een aantal UNIXen die opnemen met een vertaalde versie en bijvoorbeeld om naam en wachtwoord vragen. Als je het niet zeker weet kun je eens proberen om een naam in hoofdletters in te tikken, als hij dan "PASSWORD:" in hoofdletters vraagt dan is het een UNIX, want die schakelt automatisch naar upper case. Als je er eenmaal zeker van bent dat je een UNIX aan de lijn hebt kun je eerst eens wat standaard-logins proberen. Een lijstje staat op de volgende pagina.

root de systeembeheerder, zit er ALTIJD op en heeft alle bevoegdheden.

sysadm Superuser administratie shell, niet altijd aanwezig.

cron Process-login, regelt de tijdgebonden processen (netwerken etc.).

daemon Process-login.

games Voor spelverslaafden, soms.

bin eigenaar van systeemcommando's.

operator De operator, soms.

who geen password, geeft alleen de op dat moment ingelogde gebruikers en logt daarna weer uit.

uucp Wordt gebruikt om berichten tussen UNIXen uit te wisselen, draait geen shell (De commando interpreter), en is dus alleen bruikbaar om de MOTD (Message Of The Day) te lezen, de berichten aan alle gebruikers.

Probeer deze logins eerst met zichzelf als password, daarna gewoon gokken. Gewone gebruikers hebben vaak als login hun voornaam met daarachter een of meer letters van hun achternaam als de voornaam te vaak voorkomt. Ook afkortingen zijn populair.

Binnen, en nu?

Als je binnen bent krijg je eerst de MOTD te zien, daarna of er mail voor je is. Hierna komt er een prompt, bijvoorbeeld "$" (Dit duidt op de Bourne shell, de standaard command interpreter). Ook kan er een % teken verschijnen, dit duidt op de C-shell, een iets afwijkende versie. Als je niet tevreden bent met de huidige shell, tik dan "sh", en je krijgt de Bourne shell. Voor de beginnende gebruiker is "man [commando]" het belangrijkste commando, dit geeft namelijk bij elk gevraagde commando de manual pagina uit de UNIX Programmers Manual, het standaardwerk voor de UNIX gebruiker. (De vierkante haken gebruik ik van hier af om een argument aan te geven, dus niet letterlijk intikken).

De afzonderlijke files (programma's of tekst) liggen in directories, die bij UNIX weer in een boomstructuur onder elkaar liggen. De volledige naam van een file (dus met alle bovenliggende directories) noemen we een pathname. Voor het systeem bestaat er geen verschil tussen een tekst of een gecompileerd programma, en zelfs de directories zijn eigenlijk gewone files, ze hebben alleen een andere status. Om te zien in welke directory je je nu bevindt typ je "pwd". Als je wilt zien wat er onder de huidige directory ligt typ je "ls". Wil je meer weten dan typ je "ls -l". De "-l" noemen we een flag. Het is zeer leerzaam om de manual van "ls" eens te lezen via "man ls".

Als je 'ls -l' intikt zul je zien dat elke regel begint met een hoop onzin. Deze onzin bepaalt of het een file of een directory is en hoe deze beveiligd is. Het eerste teken geeft aan of het een directory of een file is. Directories geeft men aan met een 'd', files met '-'. De drie daarop volgende tekens geven de bevoegdheden voor de eigenaar. 'rwx' staat voor 'read', 'write', en 'execute' bevoegdheid. Is een bepaalde bevoegdheid niet aanwezig dan staat op die plaats een minnetje. Dan volgen er nog twee groepen van drie tekens, deze geven de r, w, en x bevoegdheden van resp. de groepsgenoeten van de eigenaar en alle anderen. '-rwxr-xr-x' wil dus zeggen dat het gaat om een file die voor iedereen lees- en uitvoerbaar is, maar waar alleen de eigenaar iets aan mag veranderen.

Om van directory te veranderen typ je "cd [directory]", waar directory een hele pathname is of de naam van een onderdirectory van de huidige directory."cd .." betekent een directory naar boven in de structuur. De bovenste directory geven we aan met een enkele "/".

Dan hebben we nog "cat [file]" om een file te lezen. Als er gekke dingen verschijnen was de file ofwel een gecompi-

leerd programma ofwel een directory. Het is handig om van het volgende lijstje commando's de manuals te lezen: pwd, ls, cat, ex, ed, cd, mail, who, readnews en chmod.

Met het commando "file [filenaam]" krijg je te zien wat voor type file de genoemde file (waarschijnlijk) is. Hier krijg je antwoorden als 'executable file', 'ascii text' etc.

De shell

De shell is de standaard UNIX commando interpreter, en alle commando's die we tot nu toe gehad hebben worden door de shell uitgevoerd. Het is echter mogelijk om met de file editor ("man vi" of anders "man ed") een eigen file aan te maken, en in deze file kun je dan een programma opbouwen in dezelfde syntax die je ook gewoon gebruikt, met uitbreiding van enkele loop stucturen, zoals "while .... do ..." en "if .... then ...". Zie voor uitleg "man sh" (zeer goede uitleg, en een lang verhaal) Als je eenmaal een beetje met de shell kunt werken wordt het pas echt hacken geblazen.

Maar dat alles komt aan bod in het tweede deel van deze serie, in Hack-Tic 4.

Oh ja, Uitloggen.....

Druk net zo lang op <CTRL>D totdat je de openingsmessage weer krijgt. Als dit niet werkt, typ dan "kill -9 0". Leg nooit gewoon neer, dan blijft de lijn namelijk vaak openstaan.

Bronnen:

-The UNIX Programmers Manual

-Na alle wildgroei toch standaard in zicht, Jan Bosdriesz, Computable

-Op diverse universiteiten rondhangend gespuis

• UNIX is een handelsmerk van AT&T Bell labs.

Wizard

De geinformeerde hacker heeft een Hack-Tic abonnement!

Een abonnement kost *ƒ 37,50* en duurt tien nummers. Daar de Hack-Tic ongeveer tien keer per jaar uitkomt zou je met zo'n abonnement dus een jaar verder kunnen.

Abonnee word je door het geld over te maken op bankrekeningnummer 98.72.84.541 t.n.v. Rop Gonggrijp. Heb je alleen giro, maak dan geld over naar girorekening 15368 en vermeld het bovenstaande bankrekeningnummer. Stuur tevens een briefje met naam en adres naar de redaktie: Hack-Tic, Postbus 22953, 1100 DL Amsterdam.

Abonnementen beginnen altijd met het laatste nummer, tenzij je dat anders vermeldt.

SNELHEIDSCONTROLE (bron: NEABBS) 020-717666

Volgens de laatste gegevens zijn dit de plekken waar speciale meetapparatuur van de Rijkspoltie staat opgesteld om snelheidsovertreders te pakken:

Een HACK-TIC lezerservice. Hack-Tic, Postbus 22953, 1100 DL Amsterdam.

Naam	Rijksweg	Paal
Muiden	1	12.3
Hoevelaken	1	42.8
Ughelen	1	79.0
Azelo	1	141.1
Amsterdam	2	31.6
Lage- weide	2	55.4
Zaltbommel	2	104.0
Den Bosch	2	116.7
Best	2	146.2
Maarheeze	2	180.8
Wessem	2	216.6
Roosteren	2	229.2
Maastricht	2	254.5
Burgerveen	4	18.9
Leidschendam	4	38.7
Beneluxtunnel	4	72.0
Hollandse Brug	6	45.0
Ketelbrug	6	101.7
Hoorn	7	30.3
Afsluitdijk	7	95.6
Heerenveen	7	141.8
Hoogkerk	7	187.3
Groningen	7	207.4
Gaasperdam	9	8.5
Ouderkerk	9	24.1
Velzertunnel	9	51.6
Coentunnel	10	29.3
Gouwe-aq.duct	12	26.7
Linschoten	12	46.6
Maarsbergen	12	87.8
Didam	12	147.4
Kruithuisweg	13	12.1
Botlek	15	47.3
Rhoon	15	53.3
Kesteren	15	136.7
Brienenoord	16	20.2
Drechttunnel	16	34.3
Hazeldonk	16	69.0
Maassluis	20	17.6
Rotterdam-N	20	31.4
Breda	27	9.8
Gorinchem	27	34.9
Maartensdijk	27	90.2
Zeist	28	7.4
Harderwijk	28	47.6
Zwolle	28	86.7
Staphorst	28	103.8
Spier	28	148.8
De Punt	28	189.4
Heijeoordtunnel	29	14.3
Steenwijk	32	26.1
Emmen	34	58.7
Azelo 2	35	62.1
Velperbr.lein	48	3.7
Heteren	50	161.9
Klarenbeek	50	197.0
Oirschot	58	22.7
Gilze	58	49.1
Roosendaal	58	83.5
Kruiningen	58	127.3
Oss	59	18.0
Vlijmen	59	127.6
Asten	67	48.5
Cuijk	73	88.7
Hoensbroek	76	8.3
Heijen	77	9.6
Valkenburg	79	4.7
Raalte	835	18.7
's Heerenbroek	838	8.4
Oldenzaal	844	54.3
Brienenoord	16	20.2
Drechttunnel	16	34.3
Hazeldonk	16	69.0
Maassluis	20	17.6
Rotterdam-N	20	31.4
Breda	27	9.8
Gorinchem	27	34.9
Maartensdijk	27	90.2
Zeist	28	7.4
Harderwijk	28	47.6
Zwolle	28	86.7
Staphorst	28	103.8
Spier	28	148.8
De Punt	28	189.4
Heijeoordtun.	29	14.3
Steenwijk	32	26.1
Emmen	34	58.7
Azelo 2	35	62.1
Velperbr.plein	48	3.7
Heteren	50	161.9
Klarenbeek	50	197.0
Oirschot	58	22.7
Gilze	58	49.1
Roosendaal	58	83.5
Kruiningen	58	127.3
Oss	59	18.0
Vlijmen	59	127.6
Asten	67	48.5
Cuijk	73	88.7
Hoensbroek	76	8.3
Heijen	77	9.6
Valkenburg	79	4.7
Raalte	835	18.7
's Heerenbroek	838	8.4
Oldenzaal	844	54.3

Last minute update:

Barneveld/Ede	1	54,8
Twello/Wilp	1	95,3
Veldhoven	2	159,4
Utrecht-west	2	60,0
Nieuwe-Gein Z	2	70,7
Breukelen	2	49,9
Abcoude	2	39,6
Amstelveen Z	9	25,9

Samengevat uit gegevens van o.a. de Knight Rider en Ruud Sint

BUG-REPORT

In Hack-Tic 1 is een bug geslopen. Op pagina 4 wordt gesproken over 35 gulden abonnementsgeld voor 10 nummers, in het colofon op pagina twee staat het juiste bedrag - 37,50 - vermeld.

Toen we doorhadden dat de produktiekosten bij de tamelijk kleine eerste oplagen nogal wat hoger uit zouden vallen dan we hadden berekend hebben we helaas de abonnementsgelden moeten verhogen. Door een stommiteit onzerzijds hebben we echter een vermelding van het bedrag over het hoofd gezien. Mensen die toch 35 gulden over hebben gemaakt hebben mazzel gehad (het zijn er gelukkig maar weinig geweest).

Zoals jullie wel begrijpen werkt de truuk nu niet meer. Mensen die nu 35 gulden over maken krijgen een uniek abonnement voor 9 nummers....

Spraakversleuteling politie

De politie maakt gebruik van een spraakversleutelaar die men 'crypto' noemt. Dit is de opvolger van de veel te simpele 'scramble'. Een crypto hakt de spraak in mootjes van 30 ms en gooit deze dan vakkundig door elkaar. De oudste crypto's zijn echter al bijna 20 jaar oud en toen bestonden er nog nauwelijks microprocessors.

Dus moet het probleem van de versleuteling op een simpelere manier zijn opgelost. Wie weet meer van de crypto? Heb je thuis een oude crypto en weet je niet meer wat je er mee moet? Opsturen die hap.

Je begrijpt het al: alle aanwijzingen zijn welkom! Aanwijzingen die leiden tot ontsleuteling worden zoals gebruikelijk beloond met een appeltaart. Oplossingen zenden aan de redaktiepostbus.

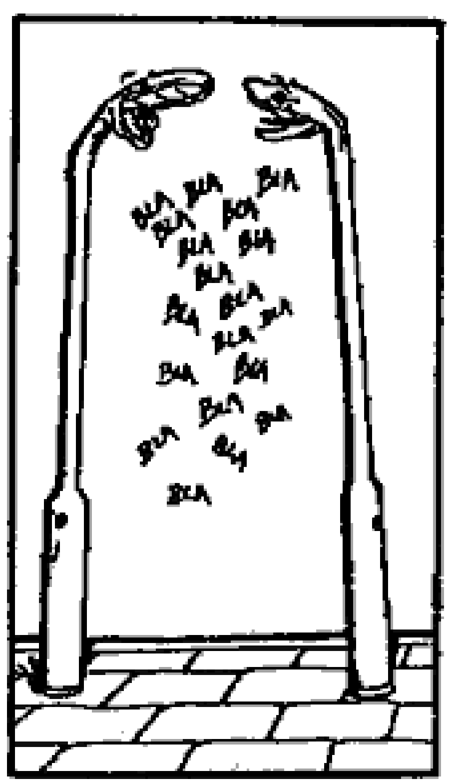
Peter Poelman

Communiceren lantaarnpalen nu ook al ?

Het is mij opgevallen dat er in de stad Utrecht en waarschijnlijk ook in andere steden kleine antennetjes aan sommige lantaarnpalen zitten. Het geheel zit op een hoogte van ongeveer 4 meter. Er zit daar een klein kastje met aan de onderkant een antennetje (gericht naar onder).

Ik denk dat het iets te maken heeft met stoplichten (ze zitten altijd in de buurt van een stoplicht) en dat de lantaarnpaal is uitgekozen zodat het antennetje hoog komt te zitten. Is er misschien iemand die mij er iets meer over kan vertellen ?

Tx.



Barcodes op auto's

Barcodes, momenteel hoodzakelijk in gebruik om levensmiddelen, boeken en god weet wat van elkaar te onderscheiden, binnenkort misschien ook benut om het verkeer op de 'harbour bridge' in Sydney wat sneller te laten stromen.

Een auto met een barcode-sticker op een van de zijruiten zou geidentificeerd kunnen worden door een lange-afstands scanner aan de kant van de weg. Als de code niet klopt wordt het kenteken alsnog gefotografeerd.

Het idee is om iedere week of maand nieuwe stickers te versturen, zolang de automobilist tenminste zijn wegenbelasting betaalt. Een ritje over de brug kost in Sydney anderhalve Aust. dollar, dus iedereen met een printer en barcode software op z'n computer kan zich daar aardig wat geld besparen.

Misschien moeten we dit eens aan Neelie voorstellen......?

Code gevonden!

In Hack-Tic 1 stond in de kort-kort-kort een artikel over een geheimzinnig nummer in Delft (015-783900). Als je dat nummer belde kreeg je een toon en kon je met je druktoetstelefoon (DTMF-toontjes) een zes-cijferige code intikken. De vraag toen was: wie vindt die code?

Het ongelofelijke is gebeurd. De code is gevonden, door ene Rico. De code was 134679 (makkelijk, kijk maar op je toetsenbordje). Echter: als je de code intikt krijg je weer een toon. Als dat even geduurd heeft (paar seconden) legt het geval neer. Wat zou hier allemaal mee kunnen? Hangt hier een outdial aan (zodat je verder kunt bellen op kosten van ....)? De vraag blijft:

Wat moet je na het ingeven van de eerste code doen?

Yooo Rico, de appeltaart is onderweg!

Anoniem ontvangen TELEFAX

Aan: HAck-Tic
betreft: *1/1989 blz 12
datum: 4 februari 1989

Hacken onder Hoogspanning

De tonen op het lichtnet zijn ongeveer 400 Hz en de amplitude is ongeveer 5 a 10% van de netspanning. Als je 5% aanbiedt moet je een vermogen leveren dat 5% is van het verbruikte lichtnetvermogen door alle aangesloten apparaten. Het is echter aanzienlijk minder, omdat het lichtnet door machine's voornamelijk inductief belast wordt. 400 Hz is 8 maal de lichtnetfrequentie, zodat er pakweg 5 maal zo weinig in het lichtnet gepompt moet worden dan bij 50 Hz nodig zou zijn. De generatoren zijn behoorlijke jongens van zo'n 50 kWatt. Peter kan dus wel vergeten zelf toontjes op het net te zetten, tenzij hij de verzegelde hoofdzekering eruit kan draaien natuurlijk maar ja, als je dat kunt hoef je ook al die moeite niet te doen want dan zit je al voor de verbruiksmeter.

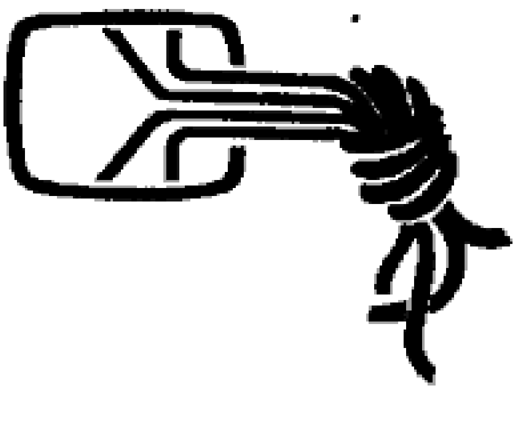
Chaos in Apeldoorn

Op de Computerdagen in Apeldoorn op 13 en 14 januari was het behoorlijk druk. Onder de vele standhouders ook de Chaos Computer Club uit Duitsland, die er in blijken te zijn geslaagd om ook buiten de Americahal waar de beurs plaatsvond de nodige drukte te veroorzaken.

De recherche van Apeldoorn heeft namelijk een persbericht van de CCC nogal serieus opgevat. Hierin had de CCC verklaard dat er vanaf de beurs wellicht enige hackpogingen zouden worden ondernomen bij bedrijven in de buurt.

In haar wijsheid besloot de recherche alle bedrijven in de omgeving die iets met computers deden te waarschuwen. Rap werd een lijst bij elkaar geveegd en namen de wakkere rechercheurs plaats achter de telefoon.

Het gerucht gaat dat een groot aantal bedrijven hun mainframes voor de gelegenheid van het telefoonnet hebben losgekoppeld. Het bekend worden van dit alles betekende voor de hack-activiteiten een flinke tegenslag, omdat het nu eenmaal moeilijk is om rustig achter je terminal te gaan zitten als je krom ligt van het lachen.



Spionnen doen aan sport.

Als je wel eens op de korte golf luistert hoor je ze wel eens, de dames die met een Duits accent komplete cijferlijsten de ether in sturen.

Dit zijn berichten voor 'spionnen in den vreemde', die deze cijfers via een kodeboek kunnen omzetten in leesbare berichten. Je hoort niet alleen cijferlijsten, maar ook komplete sportverslagen van voetbalwedstrijden die nooit gespeeld zijn en die overigens ook altijd door dames met een Duits accent worden opgelezen.

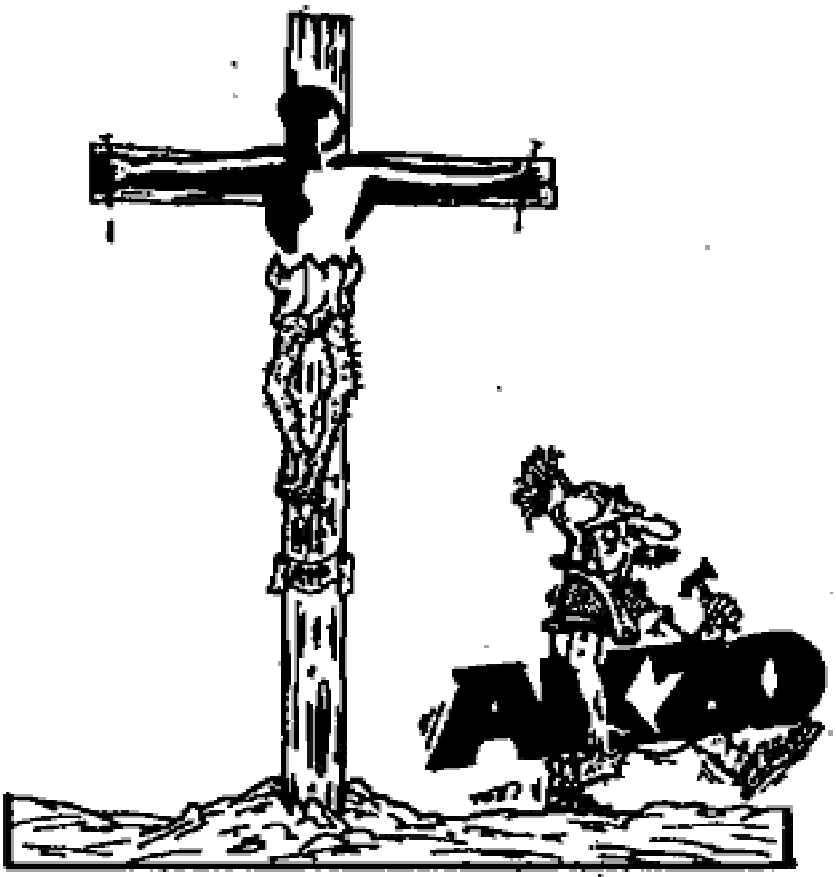
Dit accent wijst wel duidelijk in de richting van het ijzeren gordijn, of betreft het hier een rookgordijn?

kosmonauten op scanner.

Mensen die in het bezit zijn van een scanner en het luisteren naar de politie ook eens zat zijn, kunnen hun scanner eens het gebied tussen 142 en 144 MHz laten afzoeken. Hier bevinden zich verschillende frequenties die door de Russen in de ruimte worden gebruikt. De signalen die worden uitgezonden zijn vrij hard, zodat ze met een eenvoudige scanner en buitenantenne goed zijn te ontvangen. Probeer eens wat en laat ons je bevindingen weten.

Weer een computernet gekraakt

HACKZO



Sinds de PTT de gratis 060-nummers invoerde, worden deze regelmatig gescand. Een groep mensen neemt ieder een serie nummers en binnen betrekkelijk korte tijd worden ze allemaal (al dan niet machinaal) opgebeld om te kijken of er iets interessants aan hangt. Tijdens een van die scans kwamen we een nummer tegen waar een poortselector aan hing. Een poortselector is een simpele computer die niets anders doet dan doorverbinden met grotere computers, een soort data-telefoniste dus. Soms vragen deze dingen om een GROUPNAME. Meestal is dat dan de naam van een systeem en in dit geval was de groupname NET (heel origineel: van netwerk). We waren de voordeur binnen en stonden nu in de hal, vraag was alleen: wiens hal?.

Aan deze poortselector (gemaakt door DEC) bleken een heleboel verschillende systemen te hangen: VAX'en, PDP's, gateways naar andere poorten en IBM-systemen. Hoewel we nog steeds niet wisten bij wie we binnen waren was duidelijk dat de beveiliging niets te wensen overliet... voor een hacker!

Wanneer je weet met wat voor een systeem je te maken hebt, begin je met de standaard logins: USER, TEST, DEMO, en ga zo maar door. Een daarvan was raak: TEST werkte op een aantal vaxen die in een cluster opgesteld stonden in Hengelo. Niet alleen werkte test, maar deze gebruiker had ook nog FULL-PRIVS, en kon dus binnen het systeem alles doen. Bij het bekijken van een file op dit systeem kwamen we het volgende tegen:

```
$type site_info.dat
COMPANY NAME:akzo 20/20
SER NUM:12345
SUPPORT PHONE:3897
84910350 50119865 V2.31D
S2020_LOCATION:2020V231D.EXE
```

Op de tweede regel maakt de gastheer zich bekend: AKZO.......

Binnen een avond hadden we op de meeste aangesloten systemen (zowel in Hengelo, Delft, Rotterdam, als Amsterdam) eigen accounts aangemaakt en onze sporen verder gewist. Een van de eerste dingen die we altijd doen, is het runnen van het netwerkprogramma: NCP. Dan krijg je een mooi overzicht van heel het netwerk. Hiermee drongen we door naar andere systemen in Belgie, Duitsland en een stuk of twaalf andere in Nederland. Op veel systemen werkten standaardlogins met fullprivs; als dat niet meteen lukte, dan waren er altijd wel netwerkfiles te vinden met usernamen en de bijbehorende passwords. Zoiets als in het volgende fragment:

DEFINE NODE xxx TRANSMIT PASSWORD AKZOAKZO RECEIVE PASSWORD AKZOAKZO

Dit is dus een klein programmaatje dat automatisch inlogt op andere systemen, en behalve de gebruikersnaam ook het wachtwoord bevat... (Toch aardig van die mensen)

In Brussel staan ook twee systemen, met de netwerknamen BRUC02 en BRUC03. BRUC02 bleek een MICRO VAX te zijn, en ook hier werkte een standaardlogin. Tot onze verbazing kregen we het volgende op het scherm:

Main Menu
1 - Exit to DCL
2 - Log out of the SYSTEM account
3 - Invoke the MAIL utility
4 - Invoke the PHONE utility
5 - Add a user account to the system
6 - Install optional software
7 - Add or Delete a MicroVMS component
8 - Create or Modify an Autologin Terminal
9 - Back up or Restore the user files on a disk
10 - Build a Standalone BACKUP kit
11 - Set the maximum number of Interactive logins
12 - Configure the network
13 - Shut down or start up the network
14 - SHUT DOWN the system
Enter a number (? or ?# for HELP): 1

Zo kun je nog eens wat.....

Nu hanteert niet iedereen dezelfde definitie van onze hobby: de een vindt het leuk om de post en de communicatiemogelijkheden naar buiten toe te onderzoeken. De ander is meer geinteresseerd in het operating systeem op zich: hoe het werkt, hoe het in elkaar zit, wat je er wel en niet mee kunt doen. Soms is dat moeilijk, soms (te) makkelijk: de 'vaxman' verzuchtte meer dan eens: 'Hier is niks aan: stomvervelend: je kunt overal in en je hoeft nergens voor te werken. Om een idee te krijgen van het niveau van de systeembeheerders bij genoemd bedrijf, het volgende bericht:

From: AMC8::SYSTEM 30-NOV-1988
To: AZ11
Subj: how to shutdown
SHUTDOWN = = "@SYS$MGRCMD :SHUTDOWN"

Duidelijk is op welke vraag dit een antwoord is.....

Wij waren niet de enigen die op het systeem huisden: een andere 'hacker', nog erg onervaren en vooral eigenwijs had ook logins gevonden: die knul wist absoluut niet waar hij mee bezig was: hij rotzooide maar wat aan..(nog een geluk dat hij niet doorhad dat zijn logins ook fullprivs waren. Op VMS kun je dat soms niet zien met het gebruikelijke 'SHOW PROCESS/PRIVS' commando.)

In ieder geval was het gevolg, dat we na een maand of 2 onze prachtige accounts even kwijtwaren omdat de systeembeheerders nu eindelijk gemerkt hadden dat er iets of iemand bezig was geweest. Deze hacker kon hierna niet meer in de systemen komen en wij konden opgelucht ademhalen: er waren nog genoeg mogelijkheden om nog steeds met volledige privileges binnen te komen.

Na weer een maand vond hij een een andere login op een andere serie machines, die we nog niet hadden onderzocht. Deze keer met wat meer privileges en hij heeft daar zodanig huisgehouden dat AKZO de hele handel dichtgegooid heeft en nu hoogstwaarschijnlijk een ander telefoonnummer heeft op 06-0.

Toch wel jammer.

Het was de bedoeling om het systeem langzaam te verkennen. Dat kon ook gemakkelijk, want er waren accounts in overvloed. Maar na een paar dagen begonnen we ons niet zo heel prettig meer te voelen: dit netwerk was dusdanig slecht beveiligd dat het eigenlijk onverantwoord was om hier geen melding van te maken. Vooral omdat we wisten dat er op een van de nodes een pensioenfonds zat. Ook hier waren we met alle privileges binnen.

In eerste instantie dachten we er goed aan te doen de AKZO-direktie zelf te waarschuwen: maar eerdere ervaringen met dit soort bedrijven maakten dat we dit plan snel lieten vallen. Na zo'n waarschuwing is iedereen zo druk bezig elkaar de schuld te geven dat men aan het dichten van het lek helemaal niet meer toe komt.

De uitkomst van de discussie zou waarschijnlijk zijn geweest dat wij de schuldigen waren. Laat ook maar: Ze komen zichzelf vanzelf wel tegen.

De VAX/VMS heeft zeer goede beveiligingsmogelijkheden. Zowel de passwords, de directories en de files afzonderlijk kunnen extra beveiligd worden. Bovendien kun je ook heel veel netfuncties beveiligen. Onze ervaring is dat deze faciliteiten nog veel te weinig optimaal worden gebruikt. Bij AKZO bleken zelfs de meest elementaire zaken niet eens beveiligd.

Het is wellicht tekenend voor het gevoerde personeelsbeleid, en je kunt slechts hopen dat er betere mensen zitten op de verantwoordelijke plaatsen in hun chemische fabrieken.......

John D.

KNIPSELS

de Volkskrant VAN VRIJDAG 17 FEBRUARI 1989

PTT verdiende elf miljoen door foutieve berekeningen

Van onze verslaggever

AMSTERDAM — De PTT heeft in 1987 elf miljoen gulden te veel verdiend door systematisch alle lokale telefoongesprekken foutief te berekenen. De Haagse rechtbank bestempelt dit als wanprestatie in een civiele procedure, die werd aangespannen door de Algemene Nederlandse Bond van Ouderen (ANBO), de Consumentenbond en een particulier. De beide bonden concluderen uit de uitspraak dat de PTT het te veel berekende geld terug moet betalen.

Een probleem daarbij is dat de Haagse rechtbank niet wil accepteren dat ANBO en Consumentenbond zouden procederen namens alle telefoonabonnees. Voor een dergelijke bundeling van individuele belangen is, volgens de rechtbank, „in ons recht geen plaats". Daarom moet er, aldus de beide organisaties, een wettelijke regeling komen waarin ook dergelijke acties tot schadevergoeding mogelijk worden.

Daarnaast verwachten ANBO en Consumentenbond dat de geprivatiseerde PTT, die nu „klantgerichtheid" in zijn vaandel voert, de sportiviteit zal opbrengen alle abonnees financieel tegemoet te komen. Volgens de bonden mag niet worden aangenomen dat alle abonnees individueel een juridische procedure zullen aanspannen om het te veel betaalde geld terug te krijgen. De PTT bestudeert het vonnis nog en heeft voorlopig geen commentaar.

De problemen ontstonden toen de de PTT per 1 januari 1987 een lokaal tijdtarief invoerde. Dit betekende dat lokale gesprekken niet meer eindeloos konden worden gevoerd voor vijftien cent, maar dat dit bedrag per vijf minuten (tien minuten in avonduren en weekeinde) moest worden betaald.

Na enige maanden bleek op basis van klachten bij de ouderenbond en de Consumentenbond dat de eerste „tik" in werkelijkheid niet vijf of tien minuten duurde, maar zo'n 8 procent korter. Het gevolg was dat mensen die dachten binnen de vastgestelde periode te hebben gebeld, soms het dubbele moesten betalen. Uit PTT-cijfers blijkt dat het bedrijf in 1987 uiteindelijk elf miljoen gulden meer heeft ontvangen door invoering van het nieuwe tarief dan was begroot.

De PTT gaf indertijd technische redenen op voor de fout. Na dreiging met een kort geding besloot het toenmalige staatsbedrijf het publiek op de hoogte te brengen van de situatie.

De memokiezer, een veelzijdig PTT-product.

Gratis bellen in cellen



Een van de dingen die de heren technici bij de PTT hebben ontwikkeld is de memokiezer. De memokiezer is een klein, draagbaar toongeneratortje, een kastje dat piepjes maakt dus.

De tonen die het voortbrengt bij het intoetsen van een cijfer komen overeen met het geluid dat uw digitale telefoon maakt bij het intoetsen van datzelfde cijfer. Op zich al leuk, maar het beestje kan nog meer. Het is n.l. in staat om telefoonnummers op te slaan in z'n geheugen. Je hoeft het te onthouden nummer slechts 1 keer in te geven en in het vervolg zijn 2 toetsdrukken voldoende om de memokiezer het nummer van tante Truus te laten piepen. Als je tante Truus dan wilt bellen hoeft u het apparaat alleen maar tegen de hoorn te houden voordat deze (niet tante Truus) begint te piepen.

Voorwaarde is wel dat je telefoon op de digitale centrale is aangesloten.

Is dit nu zo spectaculair en een bezoekje aan de primafoon waard? Tot zover niet natuurlijk.

Maar wat gebeurt er als je naar zo'n oud model kwartjestelefoon gaat; je weet wel, die apparaten met draaischijf en zo'n venstertje, zodat u uw kwartje tot het bittere eind kunt blijven zien? Kwartje? Welk kwartje? Hoezo kwartje? Als de betreffende telefoon de pieptoontjes hoort krijgt deze spontaan een brok in z'n keel en weigert ieder kwartje door te slikken.

Dit is nu een typisch voorbeeld van een generatiekloof; het oude toestel is niet gebouwd op de moderne toonkiezers. Het oude toestel wacht totdat er een nummer **gedraaid** is met het laten vallen van kwartjes. Dit om te voorkomen dat een kies-puls wordt aangezien voor een "laat kwartje vallen-puls". Bij deze truc wordt de kiesschijf niet gebruikt, en dus wacht het toestel niet op de betaal-puls, met als gevolg dat u geen kwartjes nodig heeft om te telefoneren.

Het maakt niet uit wat of wie u belt; Washington, Chicopee, Dublin en ook de 06-koopnummers leveren geen problemen op. Het kan zijn dat deze truc bij sommigen van de lezers bekend in de oren klinkt. Inderdaad, deze truc is niet nieuw.

Reeds in 1983 werd de truc op onbekende schaal benut voor het bijhouden van (internationale) contacten. Reden voor de PTT om in 1984 te beginnen met het ombouwen van de betreffende kwartjesslikkers. Dat deze operatie veel tijd in beslag neemt, blijkt niet alleen uit een artikel in het AD van 14-1-1987, maar blijkt ook uit de praktijk van vandaag de dag.

Merkwaardig genoeg zijn er na 1983 nog cellen van dit type door PTT geïnstalleerd, maar nu alleen nog bij particulieren. Dit laatste is belangrijk omdat de verantwoordelijkheid ten aanzien van de gemaakte kosten nu bij de particulier ligt.

Deze beheert immers de cel, en krijgt zelf de rekening van de PTT. De kosten die met een memokiezer gemaakt zijn worden WEL in rekening gebracht bij de zelfstandige.

Kijk maar eens rond, je komt ze hier en daar nog tegen; in scholen, sporthallen, uitgaansgelegenheden enz., echter nooit door de PTT beheerde.

De memokiezer kost 117 Nederlandse guldens in de primafoonwinkel. Voor degenen die wat minder geld willen spenderen zijn er nog enkele alternatieven. Verreweg het eenvoudigst is het Taiwanese broertje van het PTT-product; de "Profoon Portatone" o.a. de DTK-20 (wit) en DTK-35 (goud met memoblokje) zijn voor nog geen f. 40- in de handel.

Mensen die regelmatig de NIBUD-folders lezen kunnen de toontjes van de telefoon opnemen op cassette en deze afspelen met een walkman. Degenen die zelf geen digitaal toestel hebben, kunnen de tonen ook genereren met hun (huis-) computertje volgens de volgende tabel:

	1209 Hz	1336 Hz	1477 Hz
697 Hz	1	2	3
770 Hz	4	5	6
852 Hz	7	8	9
941 Hz	*	0	#

Voorbeeld: 6=1477 Hz + 770 Hz

Het moge duidelijk zijn dat PTT-telecom hier iets niet goed heeft gedaan. Ik moet nog altijd lachen als ik weer zo'n PTT uitspraak hoor van: "Niets aan de hand, ons systeem is waterdicht, er kan niet mee worden geknoeid, de nota's kloppen", zoals onlangs nog in de krant stond.

Paul

Autotelefoonnet 2 ook niet veilig!

Toen het eerste autotelefoonnet 'vol' was (te veel abonnees en hackers op te weinig kanalen) werd het tweede in gebruik gesteld. Dit tweede net werkt met hogere frequenties (ergens rond de 400 MHz) en is volgens PTT woordvoerders 'onkraakbaar'.

Dit komt omdat de centrale behalve een telefoonnummer ook nog een 'supergeheime' apparaatcode wil 'horen'. Als deze twee niet bij elkaar horen kan er niet gebeld worden.

De verschillen tussen ATF1 en ATF2 voor de leek:

ATF1:

-"Hallo centrale, hier nummer 43256, ik wil bellen met 020-717666."

-*"Nou, dat is goed joh, komt er aan"*

ATF2:

-"Hallo centrale, hier 23416, ik wil bellen met 020-717666."

-*"Wat is je supergeheime apparaatcode?"*

-"Eh... 3175284222"

-*"Ok, komt er aan"*

Bedenk dus dat die apparaatcode bij ATF2 ongecodeerd door de ether wordt geschreeuwd. Met een beetje verstand van hoogfrequent en een beetje compukennis moet je met deze hint een eind kunnen komen.

Verder zijn er ATF2 toestellen waar je allerlei leuke grapjes kunt uithalen met EPROMmetjes, maar dat zoek je zelf maar uit.....

L.

Boeken

Steven Levy

HACKERS - heroes of the computer revolution
New York 1985,
ISBN 0-440-13405-6

Hoewel 448 pagina's dik toch een boek dat je niet makkelijk weg legt als je er in bent begonnen. Het verhaalt over de begintijd van hacking, het ontstaan van een nieuwe filosofie.

Het boek is eigenlijk opgespiltst in drie delen. Het eerste en grootste deel gaat over de zestiger jaren. Hackers hangen dan (hoofdzakelijk 's nachts) rond bij de TMRC, de Tech Model and Railroad Club aan het Massachusetts Institute of Technology (MIT). Hier hebben ze een oude telefooncentrale in gebruik genomen om een modelspoorbaan te besturen.

Toen op het MIT de TX-0 computer arriveerde schoof de club hackers meer en meer over naar de 'echte' computer. 's Nachts werd er echt geprogrammeerd. de hackers schreven debuggers, assemblers, compilers, games en meer voor de TX-0. Veracht door de officiele technici speelden de hackers met de techniek.

Overdag werd de computer gebruikt door 'Officialy Sanctioned Users', de officiële gebruikers die de computer gebruikten om saaie tabellen door te rekenen en die absoluut geen respect op konden brengen voor de ongeorganiseerde levens- en programmeerstijl van de hackers.

Tussen de studenten is ook een vreemde eend in de bijt. Peter Deutsch is 12 als hij voor het eerst met de TX-0 speelt en al snel is hij een geoefend programmeur. Dit tot wanhoop van de Officialy Sanctioned Users die er niet van houden op hun vingers gekeken (en verbeterd) te worden door een jongetje van 12.

In het eerste deel is ook de hackersethiek terug te vinden. Deze is door Levy teruggebracht tot zes basisregels.

- **Toegang tot computers - en alles wat je iets kan leren over de manier waarop de wereld in elkaar zit - moet volledig en allesomvattend zijn. Er bestaat geen techniek waar je niet met je handen aan mag zitten!**
- **Alle informatie moet gratis zijn**
- **Wantrouw autoriteit - Streef naar decentralisatie**
- **Hackers moeten op grond van hun hacking worden beoordeeld, niet op onzincriteria als opleiding, leeftijd, ras of maatschappelijke positie**
- **Je kunt met een computer Kunst en schoonheid scheppen**
- **Computers kunnen je leven ten goede veranderen**

Het tweede deel van het boek gaat over de zeventiger jaren, over de idealen van de HCC, wat stond voor de Homebrew Computer Club. Deze club geloofde in de home-computer, zij vonden dat ieder mens recht had op zijn eigen computer. Dit deel behandelt onder (veel) meer het bouwen van de Apple II in een garage door Wozniak en Jobs. Het is leuk om te lezen dat Steve Jobs, die nu als rasechte yuppie door het leven gaat, vroeger een echte hippie was, compleet met baard en oosterse filosofie.

Dan volgt nog een deel over de tachtiger jaren, onder andere handelend over de 'game hackers', IBM-PC's en de 'boom' in home-computers.

Dit boek **MOET** je gelezen hebben!

ROP

Kraak (in) de Nieuwe Revu!

"Computerkrakers bellen gratis", zo schrijft Rene de Vos in de Nieuwe Revu. Het artikel opent met een meer dan paginagrote foto van Paul Dinissen die een PTT memokiezer voor de hoorn van een kwartjesslikker met venster houdt.

Het artikel gaat verder met het commentaar van een dansschoolhouder die op deze manier is benadeeld: "Ik vind het wel behoorlijk onfatsoenlijk van de PTT."

Het verhaal spitst er een beetje op toe dat de PTT al in '84 wist dat er iets mis was en die cellen daarna nog doodleuk plaatste bij particulieren.

Opmerkelijk wordt het als onder een foto van Herschberg, Paul, Frank en Taco staat: "Computerveiligheid-expert professor Herschberg en zijn krakers". Op deze foto zit Herschberg op een kast met computerspul en tillen Paul en Frank samen Taco van de vloer.

Op deze uitleg is van de kant van de geinterviewden de nodige kritiek:

Paul: "Ik ben Prof. Herschberg z'n kraker niet, ik werk niet in opdracht van anderen."

Taco: "Wat daar allemaal instaat daar klopt niets van. Een aantal uitspraken is volledig verdraaid. Men ziet kennelijk Herschberg graag als de grote baas van alle hackertjes. Alsof hackers niet in staat zouden zijn hun eigen boontjes te doppen."

Frank: "Het is natuurlijk gedeeltelijk waar (...) Maar Herschberg geilt natuurlijk waanzinnig op die publiciteit (...) Ze hebben een aantal dingen door elkaar gehaald."

Nog leuker wordt het als het blad verhaalt van een verandering die aangebracht zou zijn in de Washington Post. Het blad rept van een fakebericht over rassenonlusten in de Punjab, geplaatst door Paul.

Paul: "ik heb nooit gezegd dat er daadwerkelijk veranderingen in de Washington Post zijn aangebracht, dat heeft die journalist uit z'n duim gezogen."

Dan duikt ook nog een mysterieuze Toon N. op in het artikel. Dit is een pseudoniem (en anagram) van Onno Tijdgat. Deze Tijdgat heeft ooit met veel rumoer het hack-wereldje (moeten) verlaten na het verkopen van andermans hack aan een computerblad.

Herschberg zegt aan het slot van het artikel nog: "Hackers zijn bijzonder nuttig, mits ze hun kennis netjes hebben toegepast. Daarom bied ik ze bescherming en adviezen."

En voor wie zouden die computerkrakertjes nou toch nuttig zijn?

ROP



Electronische schakeling maakt fraudeurs het leven gemakkelijk

Het relais, met U op één lijn.

De Telegraaf van zaterdag 28 januari brengt in een lang artikel een kort bericht: Als je het wilt en je hebt geen normbesef, dan kun je moeiteloos gebruik maken van de telefoonlijn van andere mensen door eenvoudig binnen te stappen in de betonnen huisjes, waarvan sleutels kennelijk circuleren in dubieuze kringen. Een aanzienlijke groep mensen is hier, volgens het bericht, al het slachtoffer van geworden. Ons was echter niet duidelijk hoe we dit bellen op andermans rekening moesten voorstellen; zat zo'n crimineel eenvoudig in zo'n huisje te bellen? Dat zou toch op moeten vallen....

Volgens een anonieme informant uit de 'telecommunicatiewereld' weet de PTT perfect hoe de vork in de steel zit. Ze weigert de slachtoffers schadeloos te stellen om te voorkomen dat de truuk uitlekt. Technisch zit het als volgt:

In de betonnen B20 huisjes van de PTT (dit zijn die huisjes met puntdak die door heel Nederland zijn opgesteld) bevindt zich een kabelverdeler. Iedereen in die wijk die telefoon heeft, heeft een kabel naar de verdeler. De telefooncentrale heeft naar de verdeler een hele stapel lijnen. In de verdeler wordt dit alles op een groot klemmenbord met soldeerverbindingen in orde gemaakt, zodat ze niet voor elke nieuwe lijn een draad naar de centrale hoeven te trekken.

In deze huisjes zijn ook nog een soldeerbout (bepaald niet het SMD type...) en een telefoon aanwezig. Deze telefoon hangt aan een speciaal vrijgehouden dienstlijn. Aan deze dienstlijn hing men de relaisschakeling.

"Je belt de dienstlijn (het nummer staat op de telefoon). De schakeling neemt onmiddellijk de telefoon op. Maar niet alleen dat: hij neemt ook aan de andere lijn op en verbindt deze twee over een trafo met elkaar door. Deze andere lijn kan elke lijn (dus ook jouw lijn!) in het huisje zijn. De opbeller hoort dan de kiestoon van deze andere lijn en kan door middel van DTMF (TDK) pieptoontjes verder bellen.

Deze pieptoontjes komen uit de moderne TDK druktoetstelefoons of uit toonkiezertjes die je in elke telefoonwinkel kunt kopen. De uitbellende lijn moet wel op een moderne centrale met toonkiesmogelijkheid zijn aangesloten.

De opbeller betaalt dus alleen de kosten voor het gesprek naar het huisje, de eigenaar van de uitgekozen lijn (het slachtoffer dus) de kosten van het huisje naar de uiteindelijke bestemming van het gesprek. Zolang de schakeling actief is, is het toestel van de rechtmatige eigenaar van die lijn uitgeschakeld. Hef je de verbinding met het huisje op dan herstelt zich de normale toestand."

Deze schakeling heeft zoals je misschien wel begrijpt een groot aantal toepassingsmogelijkheden. Overal waar twee telefoonlijnen aanwezig zijn kun je deze schakeling gebruiken om op kosten van de eigenaar van de uitbellende lijn verder te bellen.

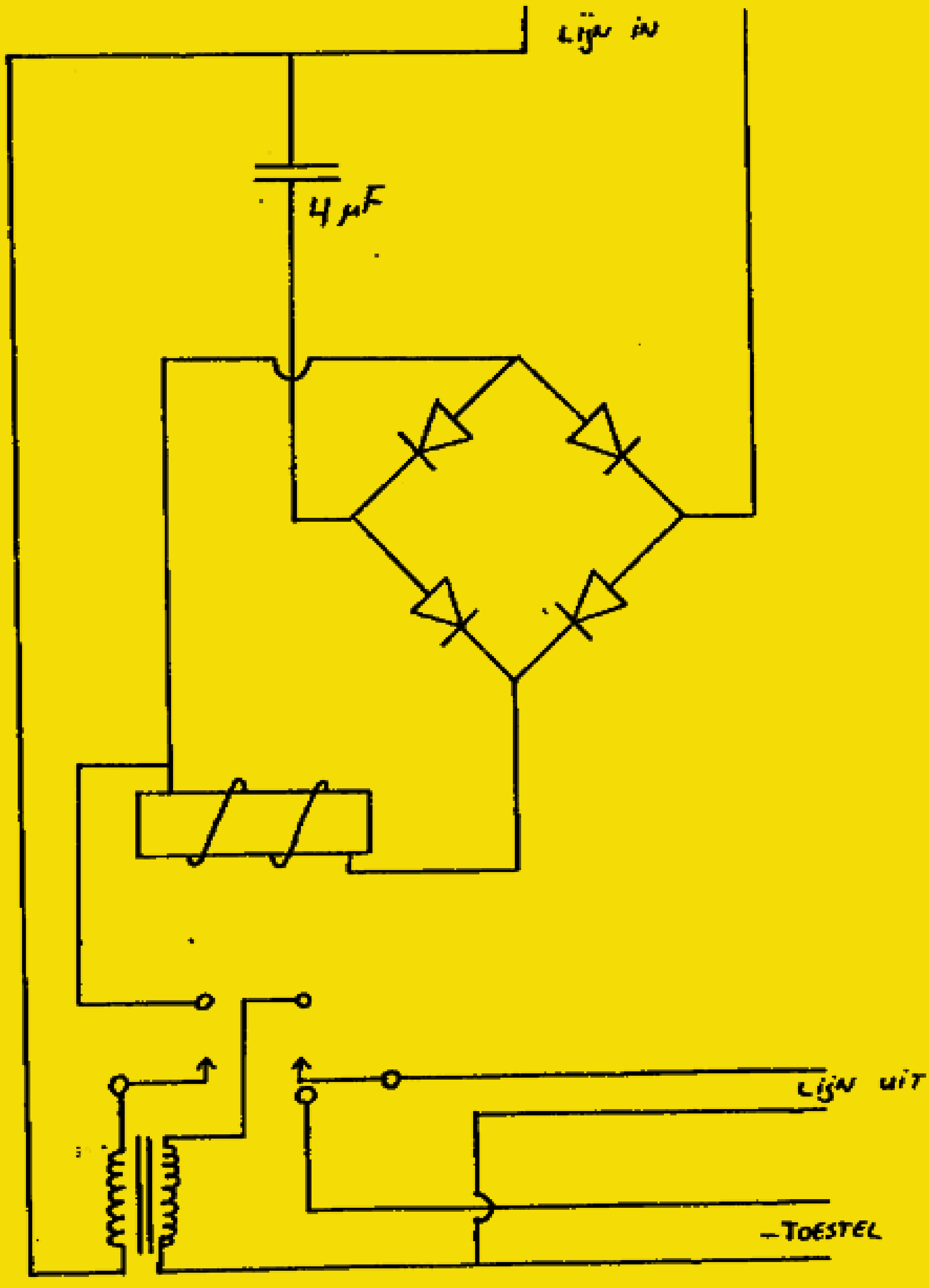
Hoewel de schakeling geniaal is in zijn eenvoud, toch enig commentaar. Als je de 'uitschakel'-optie gebruikt om het toestel van de rechtmatige eigenaar uit te schakelen wanneer je van zijn lijn gebruik maakt, 'pingt' dit toestel even voor en na je gesprek doordat de normaal op de lijn aanwezige lijnspanning wegvalt en weer terug komt.

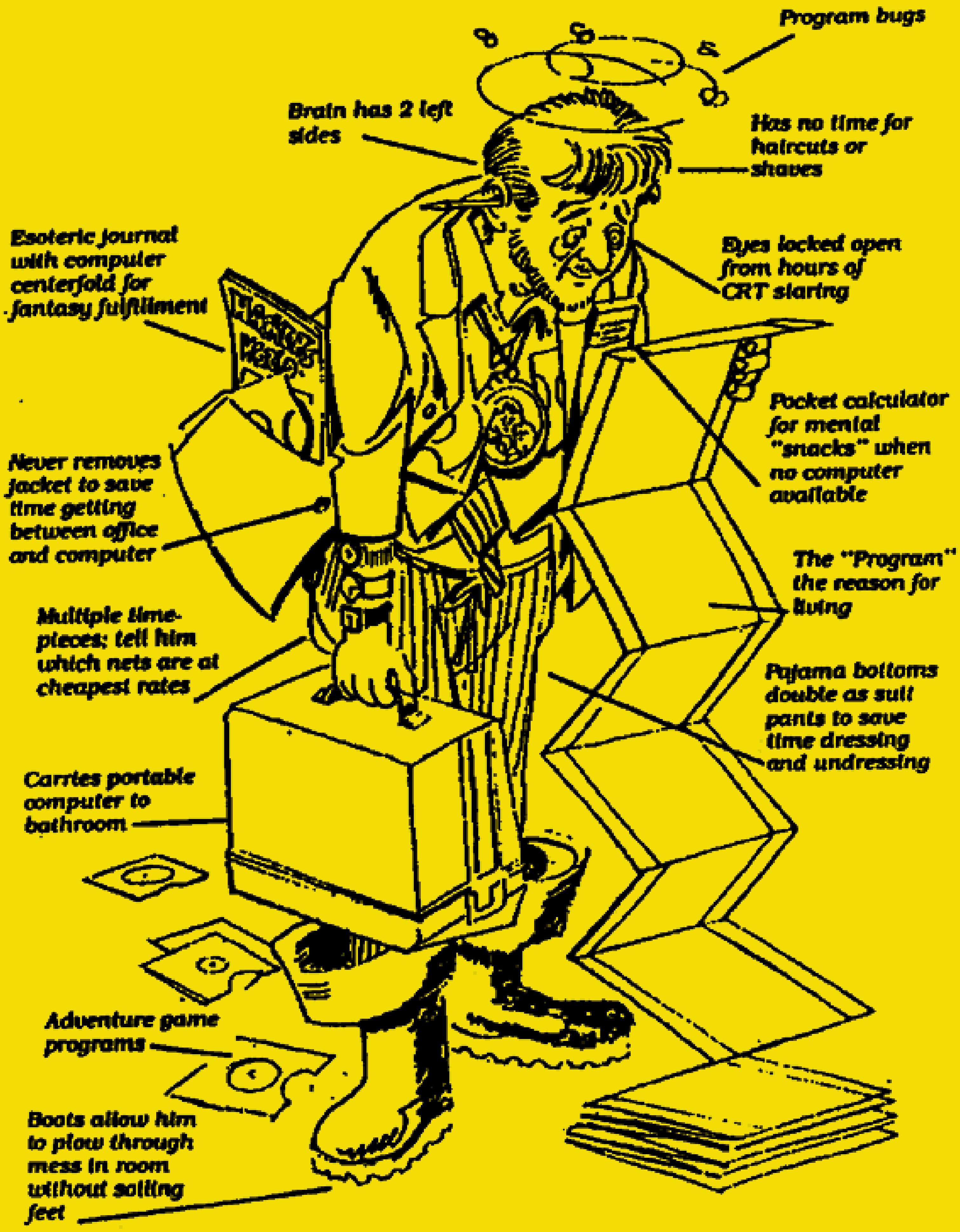
Het schema is tamelijk simpel. De diode's luisteren niet zo nauw, dat mag alles zijn. De trafo is een kwestie van uitproberen, soms is het signaal te zwak, soms pikt ie de lijn niet op.

Goede resultaten kun je behalen met een 2 x 12 V trafo, en dan de twee secundaire spoelen in serie schakelen. Nogmaals, uitproberen is hier het motto.

Als de schakeling het niet doet heb je waarchijnlijk de inkomende telefoonlijn verkeerd om aangesloten: omdraaien doet wonderen.

Het relais is heeft een schakelspanning van 12 V, en schakelt 2 maal om.




Program bugs
Brain has 2 left sides
Has no time for haircuts or shaves
Esoteric journal with computer centerfold for fantasy fulfillment
Eyes locked open from hours of CRT staring
Pocket calculator for mental "snacks" when no computer available
Never removes jacket to save time getting between office and computer
The "Program" the reason for living
Multiple time-pieces; tell him which nets are at cheapest rates
Pajama bottoms double as suit pants to save time dressing and undressing
Carries portable computer to bathroom
Adventure game programs
Boots allow him to plow through mess in room without soiling feet